

-10-

REMARKS

The Examiner has rejected Claims 1-7, 9-12, 14-21, 23-26, 28-33 under 35 U.S.C. 103(a) as being unpatentable over Kephart et al. (U.S. Patent No. 5,613,002) in view of Wells (U.S. Patent No. 6,338,141) and Albrecht (U.S. Patent Application Publication 2001/0005889). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove.

With respect to independent Claims 1, 15 and 29, the Examiner has relied on the following excerpt from Kephart to make a prior art showing of applicant's claimed "allowing access to the data if the data is successfully compared to the fingerprints of innocent data."

"If the comparison finds the checksum of the trial reconstruction and the original host checksum to be equal, the trial reconstruction is output as the original data." (Col. 5, lines 33-36)

Applicant asserts that Kephart simply discloses allowing access to data that has been reconstructed after a virus was found (see Col. 5, lines 18-22 from Kephart), such that the trial reconstruction is output as described in the excerpt above. Applicant, on the other hand, claims allowing access to the data if the data has been successfully compared to "the fingerprints of innocent data" (emphasis added). Thus, applicant's claimed data has been determined to be innocent (i.e. not having a virus, etc.), and access can be safely given to such subject data. To further clarify the difference between applicant's "data" and "innocent data," applicant has amended "data" to include "subject data" in each of the applicable claims, so as to emphasize that access is given to the subject data if the "subject data is successfully compared to the fingerprints of innocent data" (emphasis added).

Further, the Examiner has relied on the following excerpt in Albrecht to make a prior art showing of applicant's claimed "transmitting information to a server for analysis

-11-

purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data" (see independent Claims 1, 15 and 29).

"Fig. 3 illustrates the data exchange process which takes place at the application level, between the agent application and the scanning engine application, following the identification at the agent of a file which requires virus scanning. The agent initiates the FNP dialogue by sending an Initiate Negotiation request to the scanning engine. This request may include, for example, an identification of the type of file to be scanned. Using the received information, the scanning engine determines which portions of the identified file it requires in order to perform the virus scan. For example, the scanning engine may determine that it requires only the template bits at the top a Word™ file. The required portions are identified in a Request File Portions message which is sent to the agent." (Pg. 3, paragraph 0047)

The above excerpt from Albrecht teaches sending information for use in determining which portions of a file are required in order to perform the scan. Applicant asserts that this does not meet applicant's claimed "transmitting information to a server for analysis purposes if the data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data" (emphasis added). Simply nowhere in Albrecht is there any suggestion of further sending and analyzing information based such a specific condition, namely if the data has not been successfully compared to the virus definitions and the fingerprints of innocent data.

To further clarify applicant's claimed "analysis" of such data in the claimed context, applicant has amended independent Claims 1, 15 and 29 to include "wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent." Thus, when the subject data has not been successfully compared with both a virus definition and a fingerprint of innocent data, information is transmitted to a server in order to further determine whether the subject data is malicious or innocent by utilizing a virus detection algorithm.

In addition, applicant has amended independent Claims 1, 15 and 29 to incorporate the claim language of dependent Claims 4 and 5 in order to further

-12-

distinguish the “information” that is transmitted to a server for analysis purposes. Specifically, such information is now required to include at least one of “the subject data” or “a fingerprint associated with the subject data.” Therefore, the information is either the subject data itself, or a fingerprint associated with the subject data, that may be scanned by a virus detection algorithm to determine whether the subject data is malicious or innocent.

The prior art relied on by the Examiner to reject the subject matter of dependent Claims 4 and 5 (now incorporated into each of the independent claims) simply discloses allowing a file transfer if no virus is detected by utilizing virus signatures (see pg. 3, paragraph 0048 et al.). Applicant thus respectfully asserts that defining the information to be transmitted to a server for analysis purposes as “at least one of the subject data and a fingerprint associated with the subject data” clearly distinguishes over the cited prior art, especially in view of the fact that such information is sent when the subject data has not been successfully compared with both a virus definition and a fingerprint of innocent data.

With respect to independent Claim 30, applicant respectfully asserts that such claim language is allowable over the prior art for substantially the same reasons as given above for independent Claims 1, 15 and 29. Further, Claim 30 also requires “reporting that the data is innocent if the data is successfully compared to the fingerprints of innocent data,” which further distinguishes the prior art of record.

To make a prior art showing of such language, the Examiner relies on Albrecht’s disclosed “[i]n the event that no virus has been identified in the file, the agent allows the file transfer (or other operation involving the scanned file) to proceed” (see pg. 3, paragraph 48). Simply allowing a process on a file to proceed if no virus has been found from a scan simply does not meet applicant’s claimed reporting data to be innocent if the data is successfully compared to the fingerprints of innocent data. Applicant is claiming reporting, which Albrecht does not disclose, in addition to reporting based on a

-13-

successful comparison between the data and fingerprints of innocent data, not just a scan for viruses, as disclosed in Albrecht.

With respect to independent Claim 31, applicant argues that such claim language is, at least in part, deemed allowable for the reasons as argued with respect to independent Claims 1, 15 and 29. With regard to the claim language in Claim 31 (and not necessarily existent in independent Claims 1, 15 and 29), the Examiner relies on Albrecht's disclosed "the scanning engine determines which portions of the identified file it requires in order to perform the virus scan" and "the agent returns the requested portions to the scanning engine...whereupon the scanning engine commences the virus scanning operation" (see pg. 3, paragraphs 48-49) to make a prior art showing of applicant's claimed "requesting the data from the client computer utilizing the network upon an unsuccessful comparison of the fingerprint associated with the subject data and the fingerprints associated with the innocent data and the virus definitions at the server; receiving the data transmitted from the client computer in response to the request; analyzing the data transmitted from the client computer."

Applicant respectfully asserts that Albrecht fails to teach "requesting data...upon an unsuccessful comparison of the fingerprint associated with the subject data and the fingerprints associated with the innocent data and the virus definitions at the server." Albrecht, on the other hand, teaches "[t]he agent initiates the FNP dialogue by sending an Initiate Negotiation request to the scanning engine. This request may include, for example, an identification of the type of file to be scanned." (see pg. 3, paragraph 47). Thus, in Albrecht the agent simply initiates the virus scan, whereas applicant claims analyzing the data only after an unsuccessful comparison has been made between the fingerprint associated with the subject data and the fingerprints associated with the innocent data and the virus definitions at the server.

With respect to independent Claims 32 and 33, applicant asserts that such claim language distinguishes the prior art of record, at least in part, for the same reasons as argued with respect to Claim 31 et al.

-14-

It is further noted that the Examiner's application of the prior art is further deficient with respect to the dependent claims. For example, with respect to dependent Claim 3, the Examiner relies on Kephart's disclosed "the trial reconstruction is output" (col. 5, lines 33-36) to make a prior art showing of applicant's claimed "reporting that the data is innocent if the data is successfully compared to the fingerprints of innocent data." Applicant respectfully asserts that outputting data that has been reconstructed from what was previously infected data, as Kephart teaches, does not meet applicant's claimed reporting data as innocent, such that the subject data is determined not to be infected, if the data is successfully compared to the fingerprints of innocent data.

With regard to dependent Claim 10, the Examiner relies on Albrecht's disclosed process of operations when a virus is identified. Specifically, Albrecht discloses, "if no disinfection procedure is available, the file transfer procedure is suspended and the network administrator alerted, e.g. by sending a message over the network from the agent to the network administrator's workstation" (see pg. 3, paragraph 49). In Claim 10, applicant claims "analyzing the data transmitted to the server." Applicant respectfully asserts that analyzing, as claimed by applicant, clearly distinguishes alerting an administrator, as disclosed by Albrecht.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

-15-

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P018/01.095.01).

Respectfully submitted,
Zilka-Kofab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100